prey | CHILETEC



NUEVA VERSIÓN · NOVIEMBRE 2026

Checklist de
Cumplimiento de la Ley de

Protección de Datos en Chile

Ley 21.719 · 11 bloques · 63 ítems accionables

Versión autorizada por la
Mesa de Ciberseguridad de CHILETEC

Prey Inc. · CHILETEC

NUEVA VERSIÓN · NOVIEMBRE 2026

Sobre esta nueva versión

Esta nueva versión nace de un trabajo conjunto con la **Mesa de Ciberseguridad de CHILETEC**. Junto a las empresas socias que la integran, revisamos uno por uno los ítems que una organización necesita para cumplir con la Ley 21.719 de protección de datos personales, con una pregunta en mente: ¿qué hay que hacer en la práctica, en el día a día?.

Para responderla conversamos con equipos de distintas industrias y con empresas de todos los tamaños, desde la pyme donde una sola persona lleva todo lo de TI hasta organizaciones con áreas dedicadas. Escuchamos dónde se traban, qué les cuesta aterrizar y qué evidencia les piden cuando alguien pregunta "¿y cómo demuestras que cumples?".

El resultado es este checklist: **11 bloques y 63 ítems** escritos en lenguaje simple, con entregables concretos al cierre de cada bloque. Está pensado para cualquier equipo de TI, sea de una persona o de veinte, y para que lo completes junto a RRHH, operaciones, ventas y quien lleve los temas legales en tu empresa.

Gracias a la Mesa de Ciberseguridad de CHILETEC y a las empresas socias por su tiempo y dedicación al tema.



Fecha clave: la ley entra en vigencia el 15 de octubre de 2027

La fecha original era el 1 de diciembre de 2026. En noviembre de 2026 el Congreso aprobó postergarla. El plazo se amplía, pero las obligaciones no cambian: el trabajo es el mismo y conviene empezarlo hoy.

Objetivo: asegurar que tu empresa cumple con los requisitos clave de la Ley N° 21.719 y evitar sanciones.

ANTES DE EMPEZAR

Cómo usar este checklist

Para quién es

Para organizaciones chilenas de cualquier tamaño e industria: desde la pyme donde una sola persona lleva todo lo de TI hasta empresas con áreas dedicadas de tecnología, seguridad o cumplimiento. Sirve a equipos de TI, gerencias, encargados de operaciones y responsables de cumplimiento que necesitan implementar la Ley 21.719 de forma ordenada.

Qué incluye

- 11 bloques temáticos con 63 ítems accionables
- Tres estados por ítem: **Sí**, **Parcialmente** y **No**
- Un **output esperado** por bloque: los entregables que deberían quedar listos
- Un glosario al final

60 a 90 minutos

para una primera autoevaluación. Complétala en equipo: el responsable del proyecto y una persona de cada área que trata datos (TI, RRHH, operaciones, ventas).

Paso a paso

1. Lee la introducción y el glosario para alinear conceptos.
2. Recorre los bloques en orden: cada uno se apoya en el anterior.
3. Marca cada ítem: **Sí** (implementado y documentado), **Parcialmente** (hay avance, falta cerrar) o **No**.
4. Para los ítems en Parcialmente o No, anota responsable, fecha objetivo y bloqueos.
5. Al cerrar cada bloque, revisa el output esperado: ¿los entregables están listos o solo declarados?
6. Repite la autoevaluación cada seis meses o ante cambios relevantes (nueva regulación, fusión, nuevo producto, una brecha).

Esta guía es un documento de buenas prácticas. No constituye asesoría legal. Para casos específicos o decisiones críticas, consulta con un abogado o especialista en protección de datos.

MAPA

Los 11 bloques

Checklist organizado en 11 bloques que cubren las distintas dimensiones del cumplimiento: gobernanza, procesos, tecnología y cultura.

#	BLOQUE	QUÉ CUBRE
01	**Gobernanza del proyecto**	Definir responsable, sponsor, presupuesto y plazos antes de empezar.
02	**Mapeo de datos personales (RAT)**	Inventariar qué datos se tratan, dónde viven y con qué nivel de riesgo.
03	**Bases de licitud**	Asignar la razón legal de cada tratamiento (contrato, consentimiento, ley, interés legítimo).
04	**Información a los titulares**	Publicar política de privacidad, avisos a empleados y consentimientos claros.
05	**Derechos de los titulares (ARCO+)**	Habilitar canal y proceso para que las personas ejerzan sus derechos.
06	**Encargados de tratamiento**	Formalizar contratos con proveedores que tratan datos (cloud, CRM, contadora, etc.).
07	**Seguridad técnica y organizacional**	Controles mínimos razonables: cifrado, MFA, respaldos, antivirus, dispositivos, accesos.
08	**Brechas de seguridad**	Plan, criterios y tiempos para responder y notificar incidentes.
09	**Transferencias internacionales**	Identificar datos que salen de Chile y aplicar salvaguardas.
10	**Documentación y registros**	Mantener evidencia viva del cumplimiento: EIPD, auditorías, versionado.
11	**Capacitación y cultura**	Entrenar al equipo en prácticas internas y reconocimiento de amenazas.



BLOQUE 01

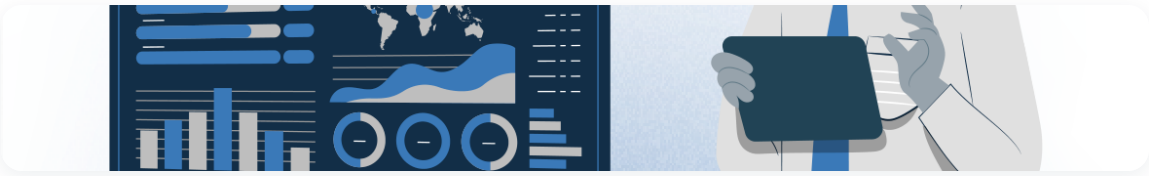
Gobernanza del proyecto

La gobernanza es el cimiento del cumplimiento. Antes de mapear datos, firmar contratos o instalar controles técnicos, hace falta definir quién lidera el proyecto, quién lo respalda desde la dirección, con qué presupuesto y en qué plazos opera. Sin esa estructura inicial, el resto del trabajo se diluye en buenas intenciones.

	ÍTEM	SÍ	PARCIAL	NO
1.1	Designar responsable interno con nombre, rol y dedicación asignada	☐	☐	☐
1.2	Definir equipo de apoyo con las áreas que tratan datos (TI, RRHH, legal, operaciones, ventas)	☐	☐	☐
1.3	Contar con sponsor de nivel ejecutivo (dueño, gerente general o directorio) que apruebe alcance y reciba reportes de avance	☐	☐	☐
1.4	Asegurar que responsable y equipo conozcan las obligaciones clave y los plazos de la Ley 21.719	☐	☐	☐
1.5	Decidir si se designará un delegado de protección de datos (DPO). La ley lo deja como opción voluntaria; en una pyme puede asumirlo el dueño o la gerencia	☐	☐	☐
1.6	Asignar presupuesto formal que cubra asesoría legal, herramientas técnicas y capacitación	☐	☐	☐
1.7	Definir cronograma con fecha de inicio, hitos clave (diagnóstico → documentación → controles → capacitación) y fecha meta anterior a la entrada en vigencia de la ley	☐	☐	☐

OUTPUT ESPERADO

- Acta de inicio firmada por el sponsor
- Plan de proyecto con cronograma e hitos
- Presupuesto aprobado
- Responsable y equipo formalmente designados
- Decisión sobre el DPO documentada
- Resumen de obligaciones clave de la Ley 21.719 compartido con el equipo



BLOQUE 02

Mapeo de datos personales (RAT)

Para cumplir la Ley 21.719 hace falta saber qué datos personales se manejan, dónde están, para qué se usan y por cuánto tiempo se guardan. A ese mapa se le conoce como Registro de Actividades de Tratamiento (RAT) y, en la práctica, es una planilla que documenta cada proceso y los datos que usa. Este bloque incluye además evaluar el riesgo de cada proceso, para priorizar controles e identificar cuáles requieren Evaluación de Impacto (EIPD).

	ÍTEM	SÍ	PARCIAL	NO
2.1	Listar los procesos de la empresa que usan datos de personas (ventas, marketing, RRHH, soporte, contabilidad, postulantes, cámaras, etc.)	☐	☐	☐
2.2	Mantener una planilla RAT con una fila por proceso: qué datos usa, de quiénes son (clientes, empleados, etc.), para qué, dónde se guardan (sistema, cloud, planillas, papel, laptops, móviles, USB) y por cuánto tiempo	☐	☐	☐
2.3	Marcar los datos sensibles (salud, biométricos, entre otros), los datos de niños, niñas y adolescentes y los tratamientos de alto riesgo (monitoreo de empleados, decisiones automatizadas)	☐	☐	☐
2.4	Evaluar el nivel de riesgo de cada proceso del RAT según probabilidad e impacto sobre los titulares, para priorizar controles e identificar cuáles requieren EIPD	☐	☐	☐
2.5	Anotar quién accede o recibe estos datos: personas dentro de la empresa y proveedores externos (contadora, agencia, soporte TI, herramientas cloud)	☐	☐	☐
2.6	Identificar datos obsoletos o duplicados para eliminarlos o anonimizarlos	☐	☐	☐
2.7	Definir responsable y frecuencia para mantener la planilla actualizada	☐	☐	☐

OUTPUT ESPERADO

- Planilla RAT llena con los procesos principales
- Datos sensibles y tratamientos de alto riesgo marcados
- Análisis de riesgo por proceso documentado
- Lista de datos obsoletos para eliminar o anonimizar
- Responsable y frecuencia de actualización definidos

Sobre el RAT: la Ley 21.719 no exige un RAT de forma explícita. Aun así, es la herramienta más útil para responder a la Agencia: te ayuda a informar a los titulares, responder solicitudes, controlar a tus proveedores, gestionar brechas y demostrar cumplimiento.



BLOQUE 03

Bases de licitud

La ley exige que cada uso de datos personales tenga una razón legal que lo respalde, llamada base de licitud. No siempre es el consentimiento: también vale un contrato con la persona (clientes, empleados), una obligación legal (SII, AFP, mutuales) o un interés legítimo justificado. Este bloque consiste en asignar a cada fila del RAT la base que mejor la justifica.

	ÍTEM	SÍ	PARCIAL	NO
3.1	Asignar una base de licitud a cada proceso del RAT, distinguiendo cuándo aplica consentimiento y cuándo otras bases (contrato, obligación legal, interés legítimo)	☐	☐	☐
3.2	Identificar los procesos que requieren consentimiento expreso (marketing, cookies no esenciales, datos opcionales, datos sensibles)	☐	☐	☐
3.3	Documentar el motivo de la base elegida en cada caso, especialmente cuando es interés legítimo	☐	☐	☐
3.4	Asegurar que los tratamientos de datos sensibles cuenten con base reforzada (consentimiento expreso o excepción legal específica)	☐	☐	☐
3.5	Revisar las bases asignadas cuando cambien procesos o se agreguen nuevos tratamientos	☐	☐	☐

OUTPUT ESPERADO

- RAT con la columna base de licitud completada por proceso
- Listado de procesos que requieren consentimiento expreso
- Justificación documentada para casos de interés legítimo
- Bases reforzadas identificadas para datos sensibles



BLOQUE 04

Información a los titulares

Las personas cuyos datos se tratan tienen derecho a saber qué se hace con su información y, cuando hace falta consentimiento, a darlo de forma libre e informada. Esto se cumple con una política de privacidad clara en el sitio web, avisos específicos por situación (empleados, postulantes, cámaras) y mecanismos de consentimiento bien implementados.

	ÍTEM	SÍ	PARCIAL	NO
4.1	Publicar política de privacidad en el sitio web, en lenguaje claro y con la información mínima (quién es el responsable, finalidades, destinatarios, plazos, derechos del titular y contacto)	☐	☐	☐
4.2	Entregar aviso de privacidad a los empleados explicando qué datos suyos se tratan y para qué (RRHH, remuneraciones, monitoreo, control de acceso)	☐	☐	☐
4.3	Implementar consentimientos claros y específicos por finalidad (sin casillas premarcadas ni “acepto todo”), guardar evidencia y dar un mecanismo simple para revocarlos	☐	☐	☐
4.4	Informar a los postulantes a empleo sobre el uso de su CV, su finalidad y plazo de conservación	☐	☐	☐
4.5	Instalar cartel visible en cámaras de seguridad que avise la grabación y su finalidad (si aplica)	☐	☐	☐
4.6	Revisar y actualizar estos avisos al menos una vez al año o cuando cambien procesos	☐	☐	☐

OUTPUT ESPERADO

- Política de privacidad publicada y accesible desde el sitio web
- Aviso de privacidad entregado a empleados
- Formularios de consentimiento ajustados, con registro y revocación
- Aviso a postulantes incorporado al proceso de selección
- Cartelería de cámaras instalada (si aplica)
- Frecuencia de revisión definida



BLOQUE 05

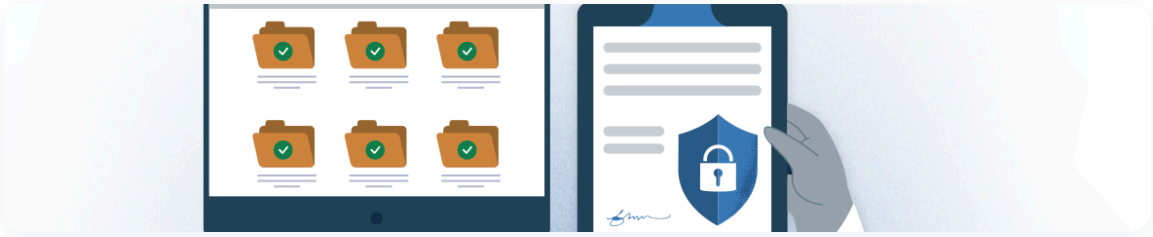
Derechos de los titulares (ARCO+)

Las personas pueden pedir acceso a sus datos, rectificarlos, suprimirlos, oponerse al tratamiento, llevárselos a otra empresa (portabilidad) o pedir que se bloquee su tratamiento mientras se resuelve su solicitud. La ley obliga a responder dentro de 30 días corridos, prorrogables una sola vez por otros 30, y a guardar respaldo de la respuesta.

	ÍTEM	SÍ	PARCIAL	NO
5.1	Establecer un canal claro y visible para que las personas ejerzan sus derechos (correo dedicado, formulario web o ambos)	☐	☐	☐
5.2	Verificar la identidad del solicitante antes de responder, para no exponer datos a quien no corresponde	☐	☐	☐
5.3	Definir cómo responder cada derecho (acceso, rectificación, supresión, oposición, portabilidad y bloqueo) dentro del plazo legal: 30 días corridos, prorrogables una vez por 30 más	☐	☐	☐
5.4	Llevar registro interno de solicitudes: quién pidió, qué pidió, plazo y respuesta	☐	☐	☐
5.5	Documentar los casos en que se puede negar legalmente la solicitud (excepciones)	☐	☐	☐
5.6	Capacitar al equipo de atención (ventas, soporte, recepción) para reconocer y derivar estas solicitudes	☐	☐	☐

OUTPUT ESPERADO

- Canal de derechos publicado (correo dedicado o formulario)
- Procedimiento de verificación de identidad documentado
- Plantillas o pasos para responder cada tipo de derecho
- Registro interno de solicitudes
- Listado de excepciones legales documentado
- Equipo de atención capacitado en derivación



BLOQUE 06

Encargados de tratamiento

Cualquier proveedor que trate datos personales por cuenta de la empresa es un encargado de tratamiento: CRM, mailing, cloud, contadora externa, agencia de marketing, soporte TI. La ley pide elegir bien a estos proveedores y formalizar la relación por contrato. Si una herramienta filtra datos, la responsabilidad sigue siendo de tu empresa.

	ÍTEM	SÍ	PARCIAL	NO
6.1	Identificar a todos los proveedores que tratan datos personales por cuenta de la organización (cloud, CRM, mailing, contadora, agencia, soporte TI, remuneraciones, etc.)	☐	☐	☐
6.2	Firmar contrato con cada encargado, incluidas las herramientas cloud y SaaS, con las cláusulas mínimas de protección de datos	☐	☐	☐
6.3	Verificar si los encargados subcontratan a otros (subencargados) y conocer esa cadena	☐	☐	☐
6.4	Evaluar la seguridad básica de los encargados antes de contratarlos (DPA disponible, certificaciones, prácticas razonables)	☐	☐	☐
6.5	Reevaluar el cumplimiento de los encargados al menos una vez al año	☐	☐	☐

OUTPUT ESPERADO

- Listado actualizado de encargados de tratamiento
- Contratos firmados o DPA aceptados con cada uno
- Mapa de subencargados conocido
- Criterio interno de evaluación de proveedores documentado
- Frecuencia de revisión definida

BLOQUE 07

Seguridad técnica y organizacional

La Ley 21.719 exige aplicar medidas de seguridad técnicas y organizativas apropiadas al riesgo. No define una lista cerrada: pide lo razonable según el tipo de datos y el tamaño de la organización. Como punto de partida, ese mínimo incluye cifrar equipos, usar contraseñas fuertes con doble factor, tener respaldos que funcionen, defenderse del malware y gestionar bien los dispositivos y los accesos.

	ÍTEM	SÍ	PARCIAL	NO
7.1	Activar cifrado de disco en los equipos con datos personales (BitLocker en Windows, FileVault en macOS)	☐	☐	☐
7.2	Aplicar autenticación robusta en sistemas críticos: contraseñas únicas en un gestor de contraseñas y doble factor (MFA) en correo, CRM, banca, cloud y RRHH	☐	☐	☐
7.3	Realizar respaldos regulares, separados del sistema principal y verificados (probar que sirven para recuperar)	☐	☐	☐
7.4	Desplegar antivirus o EDR activo y actualizado en todos los equipos	☐	☐	☐
7.5	Mantener inventario de dispositivos que acceden a datos y contar con la capacidad de localizar, bloquear o borrar en remoto equipos perdidos o robados	☐	☐	☐
7.6	Aplicar el principio de menor privilegio en accesos y tener un proceso formal de salida (cierre de accesos, devolución de equipos, eliminación segura al dar de baja)	☐	☐	☐
7.7	Definir una política de uso aceptable que cubra WhatsApp, mensajería y dispositivos personales (BYOD)	☐	☐	☐

OUTPUT ESPERADO

- Cifrado de disco verificado y documentado por equipo
- MFA activado y probado en sistemas críticos
- Respaldo probado, con fecha de última verificación
- Antivirus o EDR desplegado y monitoreado
- Inventario de dispositivos con capacidades remotas habilitadas
- Procedimiento de salida documentado
- Política de uso aceptable publicada y comunicada

CÓMO TE AYUDA PREY

Prey te ayuda con los ítems 7.1, 7.5 y 7.6 desde un solo panel: inventario de equipos Windows, macOS, Linux, Android, iOS y Chromebook; gestión del cifrado BitLocker en Windows; localización, bloqueo y borrado remoto de equipos perdidos o robados; y borrado de datos al dar de baja un equipo.



BLOQUE 08

Brechas de seguridad

Una brecha es cualquier incidente que compromete datos personales: laptop robado, correo enviado al destinatario equivocado, ransomware, acceso no autorizado o filtración de un proveedor. La ley no fija un plazo en horas: exige reportar a la Agencia **sin dilaciones indebidas** cuando hay riesgo razonable para los titulares. Tener el plan listo antes de que pase es la diferencia entre responder en horas o en semanas.

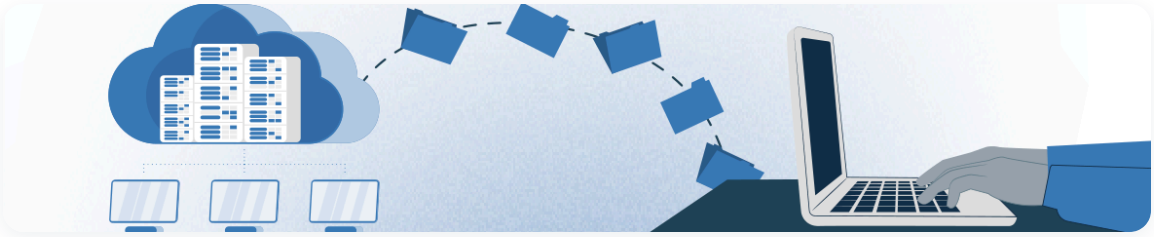
	ÍTEM	SÍ	PARCIAL	NO
8.1	Documentar un plan de respuesta a brechas con roles, pasos y plazos	☐	☐	☐
8.2	Identificar qué eventos cuentan como brecha (laptop robado con datos, correo masivo erróneo, ransomware, phishing exitoso, acceso no autorizado, filtración de un proveedor, etc.)	☐	☐	☐
8.3	Conocer los criterios de notificación: • **A la Agencia:** por los medios más expeditos posibles y sin dilaciones indebidas, si hay riesgo razonable para los titulares. • **A los titulares:** si involucra datos sensibles, de niños y niñas menores de 14 años o datos económicos, financieros, bancarios o comerciales. • **Al CSIRT Nacional de la ANCI:** si la organización es servicio esencial u OIV, alerta temprana dentro de 3 horas (Ley 21.663).	☐	☐	☐
8.4	Llevar registro interno de todas las brechas e incidentes, incluidos los que no se notifican	☐	☐	☐
8.5	Probar el plan al menos una vez (simulacro, ejercicio de mesa o revisión de un incidente real)	☐	☐	☐

OUTPUT ESPERADO

- Plan de respuesta a brechas documentado
- Criterios definidos de qué califica como brecha
- Registro interno de incidentes y brechas en operación
- Fecha del último simulacro o revisión registrada

CÓMO TE AYUDA PREY

Si el incidente es un equipo perdido o robado, Prey registra la ubicación y las acciones de bloqueo y borrado con fecha y hora. Esa trazabilidad alimenta tu registro interno (8.4) y te ayuda a mostrar que actuaste sin dilaciones indebidas.



BLOQUE 09

Transferencias internacionales

Muchas empresas chilenas transfieren datos al extranjero sin notarlo: al usar Gmail, Microsoft 365, Mailchimp, HubSpot, AWS o cualquier herramienta cloud, los datos viajan a servidores fuera de Chile. La ley no prohíbe esas transferencias, pero exige saber qué se transfiere, a dónde, con qué garantías, y declararlo en la política de privacidad.

	ÍTEM	SÍ	PARCIAL	NO
9.1	Identificar si se transfieren datos fuera de Chile (la mayoría de los servicios SaaS y cloud lo hacen: Google, Microsoft, Mailchimp, HubSpot, AWS, etc.)	☐	☐	☐
9.2	Conocer en qué países se alojan los principales servicios cloud y SaaS	☐	☐	☐
9.3	Aplicar salvaguardas adicionales cuando el país no tiene un nivel adecuado de protección (cláusulas contractuales tipo del proveedor o equivalentes)	☐	☐	☐
9.4	Informar las transferencias internacionales en la política de privacidad	☐	☐	☐
9.5	Documentar el análisis de transferencias (qué se transfiere, a dónde, base legal y salvaguardas)	☐	☐	☐

OUTPUT ESPERADO

- Listado de transferencias internacionales identificadas
- Países de alojamiento documentados por proveedor
- Salvaguardas aceptadas por escrito (DPA, cláusulas contractuales tipo)
- Política de privacidad actualizada con las transferencias
- Análisis de transferencias documentado



BLOQUE 10

Documentación y registros

La ley pide no solo cumplir, sino poder demostrarlo. Buena parte de la documentación se trabaja en los bloques anteriores (RAT, política, contratos, plan de brechas). Este bloque cubre las piezas que faltan y, sobre todo, cómo mantenerlas vivas: evaluaciones de impacto, evidencias, auditoría periódica y versionado.

	ÍTEM	SÍ	PARCIAL	NO
10.1	Realizar Evaluación de Impacto en Protección de Datos (EIPD) para los tratamientos de alto riesgo identificados en el RAT, antes de iniciarlos	☐	☐	☐
10.2	Mantener un inventario actualizado de toda la documentación del programa (política, RAT, contratos, plan de brechas, registros), con responsable y versión vigente	☐	☐	☐
10.3	Conservar evidencia de cumplimiento (consentimientos, contratos firmados, capacitaciones, comunicaciones a titulares)	☐	☐	☐
10.4	Realizar una auditoría interna o revisión del cumplimiento al menos una vez al año	☐	☐	☐
10.5	Versionar y actualizar la documentación cuando cambien procesos o salga nueva regulación	☐	☐	☐

OUTPUT ESPERADO

- EIPD realizadas para tratamientos de alto riesgo
- Inventario de documentación con responsables y versiones
- Repositorio de evidencias de cumplimiento
- Calendario de auditorías internas definido
- Procedimiento de versionado documentado



BLOQUE 11

Capacitación y cultura

La ley se cumple en la operación diaria, no en los documentos. Tu equipo es la primera línea: quien pide un consentimiento, quien envía un correo por error, quien reconoce un phishing antes de hacer clic, quien deriva una solicitud de un titular. Sin capacitación constante, todo lo anterior queda en buenas intenciones.

	ÍTEM	SÍ	PARCIAL	NO
11.1	Capacitar a todo el equipo en los conceptos esenciales de la Ley 21.719 y las prácticas internas	☐	☐	☐
11.2	Incluir protección de datos en la inducción de nuevos colaboradores	☐	☐	☐
11.3	Capacitar en reconocimiento de phishing, ingeniería social y reporte de incidentes	☐	☐	☐
11.4	Diseñar capacitación específica para los roles que tratan más datos (RRHH, ventas, soporte, TI, marketing)	☐	☐	☐
11.5	Refrescar la capacitación al menos una vez al año o cuando haya cambios relevantes (regulación, procesos, herramientas)	☐	☐	☐

OUTPUT ESPERADO

- Plan de capacitación documentado
- Capacitación inicial completada con registro
- Módulo de protección de datos incorporado a la inducción
- Capacitaciones por rol para áreas críticas
- Frecuencia anual de refresco definida



Beneficios del cumplimiento proactivo

- ✓ Reduces el riesgo de sanciones y multas.
- ✓ Mejoras la confianza de tus clientes y socios comerciales.
- ✓ Te alineas con estándares internacionales como GDPR o ISO 27001.

Lo que está en juego (Ley 21.719, art. 35)

Infracciones leves	Amonestación escrita o multa de hasta **5.000 UTM**
Infracciones graves	Multa de hasta **10.000 UTM**
Infracciones gravísimas	Multa de hasta **20.000 UTM**
Reincidencia	Hasta tres veces el monto. Si tu empresa no es de menor tamaño y reincide en una infracción grave o gravísima, hasta el **2% o 4%** de sus ingresos anuales.

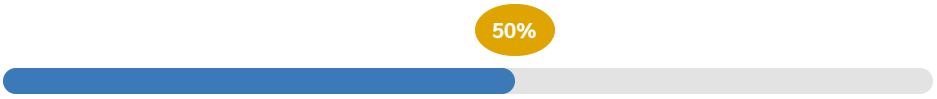
Si tu empresa es de menor tamaño (Ley 20.416): durante los primeros 12 meses de vigencia, la Agencia puede aplicar una amonestación por escrito en vez de una multa (art. sexto transitorio). Además, la Agencia fijará estándares de seguridad diferenciados según el tamaño de la empresa (art. 14 septies).

Resultado del checklist: ¿estás listo para la ley?

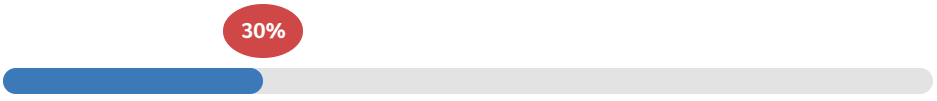
Suma 1 punto por cada **Sí** y medio punto por cada **Parcialmente**. Divide el total por los ítems que aplican a tu empresa (63 si aplican todos) y multiplica por 100.



✓ **80 a 100%** → Tu empresa está bien encaminada. Enfócate en mantener la evidencia al día.



! **50 a 79%** → Aún hay ajustes por hacer. Toma acción ahora.



✕ **Menos de 50%** → Riesgo alto de incumplimiento. Necesitas una estrategia urgente.

Qué hacer después

- Convierte los ítems en **No** en un plan de acción a 90 días.
- Convierte los ítems en **Parcialmente** en un plan a 6 meses.
- Guarda el checklist completo como evidencia de tu programa de cumplimiento.
- Comparte el resultado con tu sponsor ejecutivo y, si lo designaste, con tu DPO.

¿Necesitas ayuda? Conversa con Prey sobre protección de datos en tus dispositivos: preyproject.com/es/comenzar



Cómo Prey puede ayudarte

Varios ítems del checklist dependen de tener control real sobre los dispositivos. Prey cubre esa parte en Windows, macOS, Linux, Android, iOS y Chromebook, desde un solo panel.

- [ ] Mantenemos un inventario actualizado de los equipos que acceden a datos personales, con su hardware y software.
  Ítem 2.2 · 7.5
- [ ] Verificamos que los equipos Windows tengan el cifrado BitLocker activo.
  Ítem 7.1
- [ ] Podemos localizar, bloquear o borrar en remoto un equipo perdido o robado.
  Ítem 7.5
- [ ] Al dar de baja un equipo o cuando una persona deja la empresa, borramos sus datos de forma remota.
  Ítem 7.6
- [ ] Recibimos alertas cuando un equipo sale de una zona definida y guardamos su historial de ubicación como evidencia.
  Ítem 8.2 · 8.4
- [ ] Revisamos si correos de la empresa aparecen expuestos en filtraciones, con Prey Breach Monitoring.
  Ítem 8.2 · 11.3

¿Quieres verlo funcionando? Agenda una demo en **preyproject.com/es/comenzar**

GLOSARIO

Términos clave

En lenguaje simple, ordenados alfabéticamente.

Agencia de Protección de Datos Personales

Entidad fiscalizadora creada por la Ley 21.719. Recibe reclamos, fiscaliza el cumplimiento y aplica sanciones.

ANCI y CSIRT Nacional

Agencia Nacional de Ciberseguridad, creada por la Ley Marco 21.663. Su CSIRT Nacional recibe los reportes de incidentes de los servicios esenciales y operadores de importancia vital (OIV).

ARCO+

Nombre práctico de los derechos de las personas sobre sus datos. La Ley 21.719 reconoce el acceso, la rectificación, la supresión, la oposición, la portabilidad y el bloqueo, además del derecho a no ser objeto de ciertas decisiones automatizadas.

Base de licitud

Razón legal que justifica el uso de datos personales. No es solo el consentimiento: también aplican la ejecución de un contrato, una obligación legal, el interés legítimo y otras causales que fija la ley.

Brecha de seguridad

Cualquier incidente que comprometa los datos personales de la organización: desde un laptop robado hasta un correo enviado al destinatario equivocado, pasando por ransomware o un acceso no autorizado.

BYOD (dispositivos personales)

Práctica de usar el celular o el laptop propio para trabajar. Es muy común en pymes: el WhatsApp personal con datos de clientes es BYOD. Requiere reglas claras porque la empresa no controla esos equipos.

Consentimiento

Autorización libre, específica, informada e inequívoca que una persona da para el uso de sus datos. Las casillas premarcadas o el “acepto todo” no son consentimientos válidos.

Dato personal

Cualquier información que identifica o permite identificar a una persona: RUT, nombre, correo, dirección, teléfono, dirección IP, fotos.

Dato sensible

Categoría con protección reforzada: origen étnico o racial, afiliación política, sindical o gremial, situación socioeconómica, convicciones ideológicas o filosóficas, creencias religiosas, salud, perfil biológico, datos biométricos y vida sexual, orientación sexual e identidad de género. Los datos de niños, niñas y adolescentes tienen además reglas especiales propias.

DPA (acuerdo de tratamiento de datos)

Contrato o anexo en que un proveedor se compromete a proteger los datos que trata por cuenta de la empresa: para qué los usa, qué medidas de seguridad aplica y qué hace con ellos al terminar el servicio. La mayoría de los SaaS lo publica en su sitio.

DPO (delegado de protección de datos)

Persona que la organización puede designar para velar por el cumplimiento. La Ley 21.719 lo deja como opción voluntaria. Puede ser interno o externo, y en una pyme el dueño o la gerencia puede asumir el rol.

GLOSARIO

EIPD (evaluación de impacto)

Análisis previo a un tratamiento que puede producir alto riesgo para los titulares, para identificar y mitigar ese riesgo. La ley la exige en esos casos. También se conoce como DPIA.

Ejercicio de mesa (tabletop)

Simulacro conversado de un incidente. El equipo se reúne con un escenario, por ejemplo un laptop robado con datos de clientes, y repasa paso a paso quién hace qué, sin tocar sistemas reales.

Encargado de tratamiento

Tercero que trata datos por cuenta del responsable y bajo sus instrucciones: CRM, cloud, mailing, contadora externa, agencia de marketing.

Finalidad

Propósito específico del uso de los datos. Debe ser explícita, legítima y declarada.

RAT (Registro de Actividades de Tratamiento)

Documento que mapea cada proceso que usa datos personales, con finalidad, categorías de datos, plazos de conservación y destinatarios. La ley no lo exige, pero es la herramienta base para demostrar cumplimiento.

Responsable de datos

Organización que decide para qué y cómo se tratan los datos.

Sin dilaciones indebidas

Expresión que usa la Ley 21.719 para el reporte de brechas. No fija un número de horas: exige avisar apenas sea posible, sin demoras injustificadas. Como la rapidez se evalúa después, conviene registrar cuándo se detectó el incidente y qué se hizo en cada paso.

Subencargado

Tercero al que un encargado subcontrata el tratamiento. Ejemplo: un CRM aloja datos en AWS; AWS es subencargado.

Titular

Persona natural a la que se refieren los datos personales: cliente, colaborador, prospecto.

Transferencia internacional

Cuando los datos salen del territorio chileno. Ocurre habitualmente al usar servicios cloud o SaaS extranjeros.

Tratamiento

Cualquier operación con datos personales: recolectar, almacenar, usar, modificar, compartir, eliminar.

Sobre CHILETEC

CHILETEC es la asociación gremial de empresas tecnológicas de Chile. Representa a pequeñas, medianas y grandes empresas del sector y trabaja por su desarrollo, su competitividad y su voz ante el sector público y privado. Hace más de 20 años que impulsa el ecosistema tecnológico del país.

Mesa de Ciberseguridad

Es la instancia de CHILETEC donde las empresas socias comparten experiencia y trabajan para elevar el nivel de madurez en ciberseguridad del ecosistema, acompañando la adopción de los marcos regulatorios en ciberseguridad, datos e inteligencia artificial.

Las guías del Comité de Buenas Prácticas de la Mesa de Ciberseguridad de CHILETEC fueron desarrolladas por las empresas socias Gauss Control, Nuvo, Prey Spa y Proyecta. Esta versión, elaborada por Prey, fue autorizada por CHILETEC.

www.chiletec.org

Este documento es una guía de buenas prácticas de carácter orientador. No constituye asesoría legal, técnica ni de auditoría, y no garantiza el cumplimiento de ninguna norma ni certificación. Para casos específicos o decisiones críticas, consulta con un especialista. CHILETEC y las empresas autoras no se responsabilizan por las decisiones tomadas a partir de su contenido. La información corresponde a la normativa vigente a la fecha de publicación (noviembre de 2026) y puede cambiar; las referencias legales no reemplazan el texto de las leyes, así que verifica siempre la versión vigente en www.bcn.cl. Los recuadros y la página sobre Prey son contenido de Prey y no constituyen una recomendación ni un respaldo de CHILETEC. Las demás herramientas y proveedores mencionados son ejemplos ilustrativos.

Sobre Prey

Es una herramienta multiplataforma para el **rastreo y la seguridad** de tus dispositivos remotos. Es un servicio que actualmente protege más de 8 millones de equipos y sus datos cada día, alrededor de todo el mundo.

Prey comenzó en 2009 como una pequeña compañía de tecnología que se propuso un solo objetivo: ayudar a las personas a mantener el control de sus dispositivos. Más de 15 años después, nuestro servicio ha evolucionado hasta convertirse en una multiherramienta confiable para personas y negocios. Somos expertos en localizar, proteger y administrar tus dispositivos tecnológicos para el ocio y el trabajo. Y un equipo de personas orgullosas de poder ofrecerte apoyo.

Prey para: Personas | Organizaciones | Escuelas y Universidades

Prey Inc. ©
548 Market St. #30152
San Francisco, CA 94104
USA

Prey Spa
Av. Presidente Kennedy N°5600
Vitacura, Santiago
Chile

Todos los derechos reservados. La aplicación Prey, el logo y su marca son marcas registradas de Prey Inc. El logo de CHILETEC se usa con su autorización.